Amendments to the Claims

Claims 1 - 7 (canceled)

Claim 8 (previously presented): A computer program product for providing end-to-end user authentication for legacy host application access, said computer program product embodied on a computer-readable medium readable by a computing device in a computing environment and comprising:

computer-readable program code means for establishing a secure session from a client machine to a server machine using a digital certificate transmitted from said client machine to said server machine, wherein said digital certificate represents said client machine or a user thereof;

computer-readable program code means for storing said transmitted digital certificate at said server machine;

computer-readable program code means for establishing a session from said server machine to a host system on behalf of said client machine, responsive to establishment of said secure session, using a legacy host communication protocol;

computer-readable program code means for automatically sending a log-on message from said client machine to said server machine, responsive to receiving, at said client machine, a request from said host system for log-on information of said user, wherein said log-on message uses placeholder syntax in place of a user identifier and a password of said user;

computer-readable program code means for passing said stored digital certificate from said server machine to a host access security system, responsive to receiving, at said server machine, said log-on message from said client machine;

computer-readable program code means, operable in said host access security system, for using said passed digital certificate to locate access credentials for said user;

computer-readable program code means for returning, from said host access security system to said server machine, a user identifier associated with said located access credentials and either a stored password or a generated password substitute representing said located credentials;

computer-readable program code means for modifying, by said server machine, said received log-on message by replacing said placeholder syntax with said returned user identifier and password or password substitute; and

computer-readable program code means for forwarding said modified log-on message from said server to said host system as a response to said request for log-on information, such that said user identifier and password or password substitute from said forwarded log-on message can be used by said host system to transparently log said user on to a secure legacy host application executing at said host system, without requiring change to said host system.

Claims 9 - 16 (canceled)

Claim 17 (previously presented): A system for providing end-to-end user authentication for legacy host application access in a computing environment, comprising:

means for establishing a secure session from a client machine to a server machine using a digital certificate transmitted from said client machine to said server machine, wherein said digital certificate represents said client machine or a user thereof;

means for storing said transmitted digital certificate at said server machine;

means for establishing a session from said server machine to a host system on behalf of said client machine, responsive to establishment of said secure session, using a legacy host communication protocol;

means for automatically sending a log-on message from said client machine to said server machine, responsive to receiving, at said client machine, a request from said host system for log-on information of said user, wherein said log-on message uses placeholder syntax in place of a user identifier and a password of said user;

means for passing said stored digital certificate from said server machine to a host access security system, responsive to receiving, at said server machine, said log-on message from said client machine;

means, operable in said host access security system, for using said passed digital certificate to locate access credentials for said user;

means for returning, from said host access security system to said server machine, a user identifier associated with said located access credentials and either a stored password or a generated password substitute representing said located credentials;

means for modifying, by said server machine, said received log-on message by replacing said placeholder syntax with said returned user identifier and password or password substitute; and

means for forwarding said modified log-on message from said server to said host system as a response to said request for log-on information, such that said user identifier and password or password substitute from said forwarded log-on message can be used by said host system to transparently log said user on to a secure legacy host application executing at said host system, without requiring change to said host system.

Claims 18 - 25 (canceled)

Claim 26 (previously presented): A method for providing end-to-end user authentication for legacy host application access in a computing environment, comprising steps of:

establishing a secure session from a client machine to a server machine using a digital certificate transmitted from said client machine to said server machine, wherein said digital certificate represents said client machine or a user thereof;

storing said transmitted digital certificate at said server machine;

establishing a session from said server machine to a host system on behalf of said client machine, responsive to establishment of said secure session, using a legacy host communication protocol;

automatically sending a log-on message from said client machine to said server machine, responsive to receiving, at said client machine, a request from said host system for log-on information of said user, wherein said log-on message uses placeholder syntax in place of a user identifier and a password of said user;

passing said stored digital certificate from said server machine to a host access security system, responsive to receiving, at said server machine, said log-on message from said client machine;

using, by said host access security system, said passed digital certificate to locate access credentials for said user;

returning, from said host access security system to said server machine, a user identifier associated with said located access credentials and either a stored password or a generated password substitute representing said located credentials;

modifying, by said server machine, said received log-on message by replacing said placeholder syntax with said returned user identifier and password or password substitute; and

forwarding said modified log-on message from said server to said host system as a response to said request for log-on information, such that said user identifier and password or password substitute from said forwarded log-on message can be used by said host system to transparently log said user on to a secure legacy host application executing at said host system, without requiring change to said host system.

Claim 27 (canceled)

Claim 28 (previously presented): The method as claimed in Claim 26, wherein said digital certificate is an X.509 certificate.

Claim 29 (currently amended): The method as claimed in Claim 26, wherein said communication protocol is a 3270 ~~emulation~~ legacy host communication protocol.

Claim 30 (currently amended): The method as claimed in Claim 26, wherein said communication protocol is a 5250 ~~emulation~~ legacy host communication protocol.

Claim 31 (previously presented): The method as claimed in Claim 26, wherein said communication protocol is a Virtual Terminal protocol.

Claim 32 (previously presented): The method as claimed in Claim 26, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 33 (previously presented): A method of enabling a user at a client device to transparently log on to a legacy session with a legacy host application, without requiring change to said legacy host application, comprising steps of:

caching a digital certificate associated with said client device, or a user thereof, at a server to which said digital certificate has been provided for authentication of said client device or said user;

initiating, by said server on behalf of said client device, said legacy session with said legacy host application;

automatically responding, by said client device, to a log-on request from said legacy host application, where said log-on request is sent by said legacy host application responsive to said initiating step, by sending a log-on message in which placeholder syntax is used in place of a user identifier and password expected by said legacy host application; and

before forwarding said sent log-on message from said server to said legacy host application, performing steps of:

using said cached digital certificate to obtain, at said server from a host access security system, said expected user identifier and either said expected password or a password substitute therefor which is generated by said host access security system; and

replacing said placeholder syntax in said sent log-on message with said obtained user identifier and password or password substitute.

Claim 34 (new): The method as claimed in Claim 33, wherein said digital certificate is an X.509 certificate.

Claim 35 (new): The method as claimed in Claim 33, wherein said legacy session uses a 3270 legacy host communication protocol.

Claim 36 (new): The method as claimed in Claim 33, wherein said legacy session uses a 5250 legacy host communication protocol.

Claim 37 (new): The method as claimed in Claim 33, wherein said legacy session uses a Virtual Terminal communication protocol.

Claim 38 (new): The method as claimed in Claim 33, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 39 (new): A system for enabling a user at a client device to transparently log on to a legacy session with a legacy host application, without requiring change to said legacy host application, comprising:

means for caching a digital certificate associated with said client device, or a user thereof, at a server to which said digital certificate has been provided for authentication of said client device or said user;

means for initiating, by said server on behalf of said client device, said legacy session with said legacy host application;

means for automatically responding, by said client device, to a log-on request from said legacy host application, where said log-on request is sent by said legacy host application responsive to said means for initiating, by sending a log-on message in which placeholder syntax is used in place of a user identifier and password expected by said legacy host application; and

before forwarding said sent log-on message from said server to said legacy host application, means for performing steps of:

using said cached digital certificate to obtain, at said server from a host access security system, said expected user identifier and either said expected password or a password substitute therefor which is generated by said host access security system; and replacing said placeholder syntax in said sent log-on message with said obtained user identifier and password or password substitute.

Claim 40 (new): The system as claimed in Claim 39, wherein said digital certificate is an X.509 certificate.

Claim 41 (new): The system as claimed in Claim 39, wherein said legacy session uses a 3270 legacy host communication protocol.

Claim 42 (new): The system as claimed in Claim 39, wherein said legacy session uses a 5250 legacy host communication protocol.

Claim 43 (new): The system as claimed in Claim 39, wherein said legacy session uses a Virtual Terminal communication protocol.

Claim 44 (new): The system as claimed in Claim 39, wherein said host access security system is a Resource Access Control Facility (RACF) system.

Claim 45 (new): A computer program product for enabling a user at a client device to transparently log on to a legacy session with a legacy host application, without requiring change to said legacy host application, said computer program product embodied on a computer-readable medium readable by a computing device in a computing environment and comprising:

computer-readable program code means for caching a digital certificate associated with said client device, or a user thereof, at a server to which said digital certificate has been provided for authentication of said client device or said user;

computer-readable program code means for initiating, by said server on behalf of said client device, said legacy session with said legacy host application;

computer-readable program code means for automatically responding, by said client device, to a log-on request from said legacy host application, where said log-on request is sent by said legacy host application responsive to said computer-readable program code means for initiating, by sending a log-on message in which placeholder syntax is used in place of a user identifier and password expected by said legacy host application; and

before forwarding said sent log-on message from said server to said legacy host application, computer-readable program code means for performing steps of:

using said cached digital certificate to obtain, at said server from a host access security system, said expected user identifier and either said expected password or a password substitute therefor which is generated by said host access security system; and

replacing said placeholder syntax in said sent log-on message with said obtained user identifier and password or password substitute.

Claim 46 (new): The computer program product as claimed in Claim 45, wherein said digital certificate is an X.509 certificate.

Claim 47 (new): The computer program product as claimed in Claim 45, wherein said legacy session uses a 3270 legacy host communication protocol.

Claim 48 (new): The computer program product as claimed in Claim 45, wherein said legacy session uses a 5250 legacy host communication protocol.

Claim 49 (new): The computer program product as claimed in Claim 45, wherein said legacy session uses a Virtual Terminal communication protocol.

Claim 50 (new): The computer program product as claimed in Claim 45, wherein said host access security system is a Resource Access Control Facility (RACF) system.